INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

March 2023

The total zero-day vulnerabilities count for March month : 346

Command Injection	CSRF	Local File Inclusion	SQL Injection	XSS Injection	XXE Attack	Malicious File Upload
23	22	16	118	143	1	23

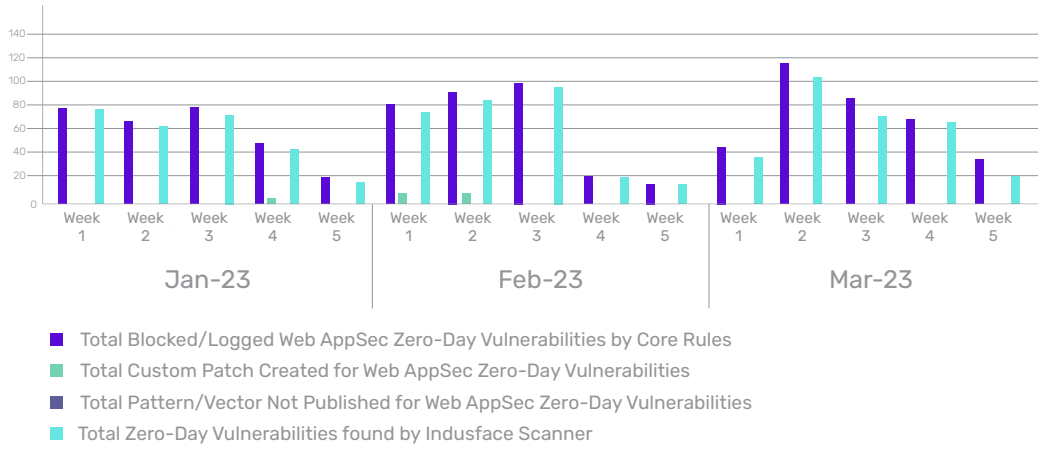
Zero-day vulnerabilities protected through core rules	346
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities for which protection can not be done	0
Zero-day vulnerabilities found by Indusface WAS	301

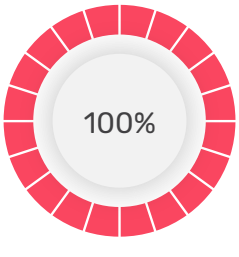
- To enable custom rules, please contact support@indusface.com
- Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

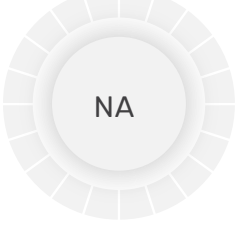
The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.

Weekly Vulnerability Trend

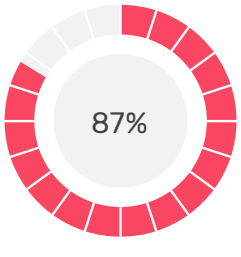




of the zero-day vulnerabilities were protected by the **core rules** in the last month.

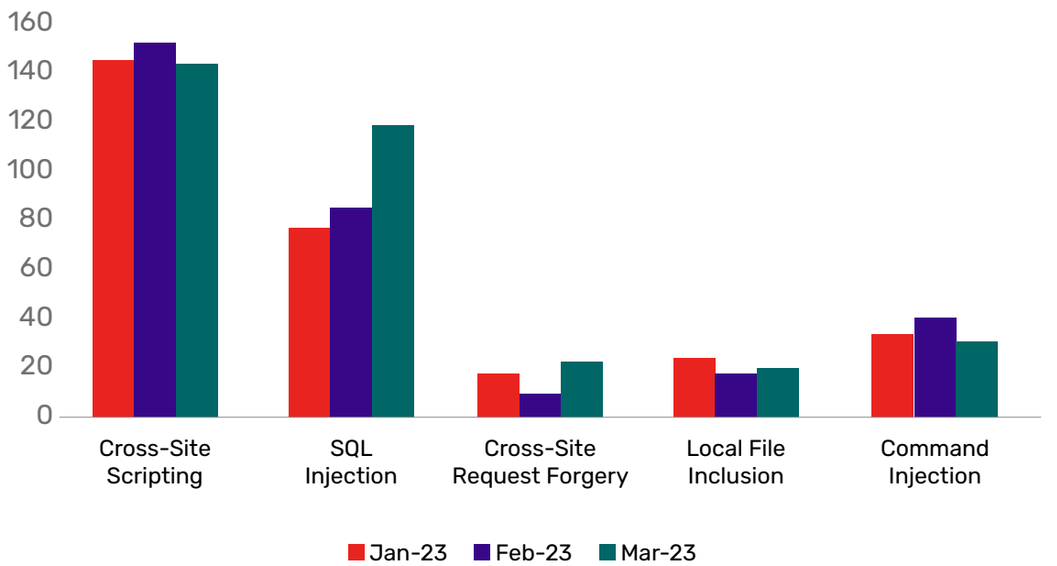


of the zero-day vulnerabilities were protected by the **custom rules** in the last month.



of the zero-day vulnerabilities were reported by **Indusface Scanner** in the last month.

Top Five Vulnerability Categories



Vulnerability Details

Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-26213	Barracuda CloudGen WAN prior 8.3.1-174141891/9.0.0 / ajax/update_certificate :: os command injection	A vulnerability classified as critical was found in Barracuda CloudGen WAN. Affected by this vulnerability is the function :: of the file /ajax/update_certificate. The manipulation leads to os command injection. This vulnerability is known as CVE-2023-26213. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-1162	DrayTek Vigor 2960 1.5.1.4 mainfunction.cgi sub_1225C command injection	A vulnerability which was classified as critical was found in DrayTek Vigor 2960 1.5.1.4. Affected is the function sub_1225C of the file mainfunction.cgi. The manipulation leads to command injection. This vulnerability is traded as CVE-2023-1162. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-26490	mailcow prior 2023-03 Sync Job os command injection (GHSA-3j2f-wf52-cjg7)	A vulnerability which was classified as critical was found in mailcow. Affected is an unknown function of the component Sync Job. The manipulation leads to os command injection. This vulnerability is traded as CVE-2023-26490. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-26107	sketchsvg shell.exec code injection	A vulnerability classified as critical has been found in sketchsvg. This affects the function shell.exec. The manipulation leads to code injection. This vulnerability is uniquely identified as CVE-2023-26107. The attack needs to be approached locally. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-1270	btcpayserver up to 1.8.2 command injection	A vulnerability which was classified as problematic was found in btcpayserver up to 1.8.2. This affects an unknown part. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2023-1270. An attack has to be approached locally. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-25395	TOTOLINK A7100RU 7.4cu.2313_ B20191024 command injection	A vulnerability has been found in TOTOLINK A7100RU 7.4cu. 2313_ B20191024 and classified as critical. This vulnerability affects unknown code. The manipulation leads to command injection. This vulnerability was named CVE-2023-25395. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-1277	kylin-system-updater up to 1.4.20kord on Ubuntu Kylin Update InstallSnap command injection	A vulnerability which was classified as critical was found in kylin-system-updater up to 1.4.20kord. Affected is the function InstallSnap of the component Update Handler. The manipulation leads to command injection. This vulnerability is traded as CVE-2023-1277. The attack needs to be approached locally. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-24762	D-Link DIR-867 1.30B07 HNAP1 SetVirtualServerSettings LocalIPAddress os command injection	A vulnerability which was classified as critical has been found in D-Link DIR-867 1.30 B07. Affected by this issue is the function SetVirtualServerSettings of the component HNAP1 Handler. The manipulation of the argument LocalIPAddress leads to os command injection. This vulnerability is handled as CVE-2023-24762. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-25279	D-Link DIR820LA1 105B03 os command injection	A vulnerability was found in DLink DIR820LA1 105B03. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to os command injection. The identification of this vulnerability is CVE-2023-25279. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-27581	github-slug-action up to 4.4.0 command injection (GHSA-6q4m-7476-932w)	A vulnerability has been found in github-slug-action up to 4.4.0 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to command injection. This vulnerability is known as CVE-2023-27581. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-28343	Altenergy Power Control Software C1.2.5 set_timezone os command injection	A vulnerability was found in Altenergy Power Control Software C1.2.5. It has been classified as critical. Affected is the function set_timezone of the file index.php /management/set_timezone. The manipulation of the argument timezone leads to os command injection. This vulnerability is traded as CVE-2023-28343. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-27240	Tenda AX3 16.03.12.11 /goform/AdvSetLanip lanip command injection	A vulnerability which was classified as critical was found in Tenda AX3 16.03.12.11. This affects an unknown part of the file /goform/AdvSetLanip. The manipulation of the argument lanip leads to command injection. This vulnerability is uniquely identified as CVE-2023- 27240. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-24229	DrayTek Vigor2960 1.5.1.4 mainfunction.cgi command injection	A vulnerability which was classified as critical was found in DrayTek Vigor2960 1.5.1.4. This affects an unknown part of the file mainfunction.cgi. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2023-24229. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-28110	Jumpserver up to 2.28.7 Koko command injection (GHSA-6x5p-jm59-jh29)	A vulnerability was found in Jumpserver up to 2.28.7. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Koko. The manipulation leads to command injection. This vulnerability is known as CVE-2023-28110. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-25280	D-Link DIR820LA1 105B03 ping.ccp ping_addr os command injection	A vulnerability was found in DLink DIR820LA1 105B03. It has been declared as critical. This vulnerability affects unknown code of the file ping. ccp. The manipulation of the argument ping_addr leads to os command injection. This vulnerability was named CVE-2023-25280. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-1389	TP-Link Archer AX21 prior 1.1.4 Build 20230219 Web Management Interface locale popen country os command injection	A vulnerability classified as very critical was found in TPLink Archer AX21. This vulnerability affects the function popen of the file /cgibin/ luci;stok/locale of the component Web Management Interface. The manipulation of the argument country leads to os command injection. This vulnerability was named CVE-2023-1389. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-37337	Netgear Orbi Router RBR750 4.6.8.5 HTTP Request os command injection (TALOS-2022-1596)	A vulnerability was found in Netgear Orbi Router RBR750 4.6.8.5. It has been classified as critical. This affects an unknown part of the component HTTP Request Handler. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2022-37337. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-27078	TP-Link MR3020 1_150921 tftp Endpoint command injection	A vulnerability which was classified as critical has been found in TP-Link MR30201_150921. This issue affects some unknown processing of the component tftp Endpoint. The manipulation leads to command injection. The identification of this vulnerability is CVE-2023-27078. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-27135	TOTOLINK A7100RU 7.4cu. 2313_ B20191024 /setting / setWanIeCfg enabled command injection	A vulnerability which was classified as critical was found in TOTOLINK A7100RU 7.4cu. 2313_ B20191024. Affected is an unknown function of the file /setting/setWanIeCfg. The manipulation of the argument enabled leads to command injection. This vulnerability is traded as CVE-2023-27135. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-28491	TOTOLink outdoor CPE CP900 6.3c.566_B20171026 Request NTPSyncWithHost host_ name command injection	A vulnerability classified as critical has been found in TOTOLink outdoor CPE CP900 6.3c.566_ B20171026. This affects the function NTPSyncWithHost of the component Request Handler. The manipulation of the argument host_name leads to command injection. This vulnerability is uniquely identified as CVE-2022- 28491. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2023-27079	Tenda G103 1.0.05 Package command injection	A vulnerability which was classified as critical was found in Tenda G103 1.0.05. This affects an unknown part of the component Package Handler. The manipulation leads to command injection. This vulnerability is uniquely identified as CVE-2023- 27079. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2022-28494	TOTOLink Outdoor CPE CP900 6.3c.566_B20171026 Request setUpgradeFW filename command injection	A vulnerability which was classified as critical was found in TOTOLink Outdoor CPE CP900 6.3c. 566_ B20171026. Affected is the function setUpgradeFW of the component Request Handler. The manipulation of the argument filename leads to command injection. This vulnerability is traded as CVE-2022-28494. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Command Injection attack
CVE-2018-25083	pullit up to 1.3.x on Node.js Git Branch Name eval os command injection	A vulnerability was found in pullit up to 1.3.x. It has been classified as critical. Affected is the function eval of the component Git Branch Name Handler. The manipulation leads to os command injection. This vulnerability is traded as CVE-2018-25083. The attack needs to be done within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Command Injection attack

Cross-Site Request Forgery Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1086	Preview Link Generator Plugin up to 1.0.3 on WordPress Plugin Activation cross-site request forgery	A vulnerability was found in Preview Link Generator Plugin up to 1.0.3 and classified as problematic. Affected by this issue is some unknown functionality of the component Plugin Activation Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-1086. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-1087	WC Sales Notification Plugin up to 1.2.2 on WordPress Plugin Activation cross-site request forgery	A vulnerability has been found in WC Sales Notification Plugin up to 1.2.2 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Plugin Activation Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-1087. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-1088	WP Plugin Manager Plugin up to 1.1.7 on WordPress Plugin Activation cross-site request forgery	A vulnerability which was classified as problematic was found in WP Plugin Manager Plugin up to 1.1.7. Affected is an unknown function of the component Plugin Activation Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-1088. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-0497	HT Portfolio Plugin up to 1.1.4 on WordPress Plugin Activation cross-site request forgery	A vulnerability was found in HT Portfolio Plugin up to 1.1.4 and classified as problematic. Affected by this issue is some unknown functionality of the component Plugin Activation Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-0497. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-0501	Insurance Service Plugin up to 2.1.3 on WordPress Activation cross-site request forgery	A vulnerability was found in Insurance Service Plugin up to 2.1.3. It has been classified as problematic. This affects an unknown part of the component Activation Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-0501. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-27490	NextAuth.js up to 4.20.0 OAuth cross-site request forgery (GHSA-7r7x-4c4q-c4qf)	A vulnerability which was classified as problematic was found in NextAuth.js up to 4.20.0. This affects an unknown part of the component OAuth Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-27490. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-27234	JIZHICMS 2.4.5 Configuration /Sys/index.html cross-site request forgery (ID 85)	A vulnerability classified as problematic has been found in JIZHICMS 2.4.5. Affected is an unknown function of the file /Sys/index.html of the component Configuration Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-27234. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-3894	WP OAuth Server Plugin up to 4.2.4 on WordPress cross-site request forgery	A vulnerability was found in WP OAuth Server Plugin up to 4.2.4 and classified as problematic. This issue affects some unknown processing. The manipulation leads to crosssite request forgery. The identification of this vulnerability is CVE-2022-3894. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-0498	WP Education Plugin up to 1.2.6 on WordPress cross-site request forgery	A vulnerability was found in WP Education Plugin up to 1.2.6. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-0498. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-0502	WP News Plugin up to 1.1.9 on WordPress cross-site request forgery	A vulnerability was found in WP News Plugin up to 1.1.9 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2023-0502. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0504	HT Politic Plugin up to 2.3.7 on WordPress cross-site request forgery	A vulnerability has been found in HT Politic Plugin up to 2.3.7 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-0504. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-0500	WP Film Studio Plugin up to 1.3.4 on WordPress cross-site request forgery	A vulnerability which was classified as problematic has been found in WP Film Studio Plugin up to 1.3.4. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-0500. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-0496	HT Event Plugin up to 1.4.5 on WordPress cross-site request forgery	A vulnerability classified as problematic has been found in HT Event Plugin up to 1.4.5. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2023-0496. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-0495	HT Slider for Elementor Plugin up to 1.3.x on WordPress cross-site request forgery	A vulnerability classified as problematic was found in HT Slider for Elementor Plugin up to 1.3.x. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-0495. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-0499	QuickSwish Plugin up to 1.0.x on WordPress cross-site request forgery	A vulnerability which was classified as problematic was found in QuickSwish Plugin up to 1.0.x. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2023-0499. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0505	Ever Compare Plugin up to 1.2.3 on WordPress cross-site request forgery	A vulnerability was found in Ever Compare Plugin up to 1.2.3. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2023-0505. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-1089	Coupon Zen Plugin up to 1.0.5 on WordPress cross-site request forgery	A vulnerability classified as problematic was found in Coupon Zen Plugin up to 1.0.5. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-1089. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-0335	WP Shamsi Plugin up to 4.3.3 on WordPress cross-site request forgery	A vulnerability was found in WP Shamsi Plugin up to 4.3.3 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to crosssite request forgery. This vulnerability is handled as CVE-2023-0335. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2023-0484	Contact Form 7 Widget for Elementor Page Builder & Gutenberg Blocks Plugin crosssite request forgery	A vulnerability was found in Contact Form 7 Widget for Elementor Page Builder & Gutenberg Blocks Plugin and Gutenberg Blocks Plugin up to 1.1.5. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2023-0484. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-0503	Free WooCommerce Theme 99fy Extension Plugin up to 1.2.7 on WordPress cross-site request forgery	A vulnerability which was classified as problematic has been found in Free WooCommerce Theme 99fy Extension Plugin up to 1.2.7. This issue affects some unknown processing. The manipulation leads to crosssite request forgery. The identification of this vulnerability is CVE-2023-0503. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2023-1093	OAuth Single Sign On Plugin up to 6.24.1 on WordPress cross-site request forgery	A vulnerability has been found in OAuth Single Sign On Plugin up to 6.24.1 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2023-1093. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0336	OoohBoi Steroids for Elementor Plugin up to 2.1.3 on WordPress cross-site request forgery	A vulnerability was found in OoohBoi Steroids for Elementor Plugin up to 2.1.3. It has been classified as problematic. This affects an unknown part. The manipulation leads to crosssite request forgery. This vulnerability is uniquely identified as CVE-2023-0336. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1112	Drag and Drop Multiple File Upload Contact Form 7 5.0.6.1 on WordPress adminajax.php upload_name path traversal	A vulnerability was found in Drag and Drop Multiple File Upload Contact Form 7 5.0.6.1. It has been classified as critical. Affected is an unknown function of the file admin-ajax.php. The manipulation of the argument upload_name leads to relative path traversal. This vulnerability is traded as CVE-2023-1112. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-1163	DrayTek Vigor 2960 1.5.1.4 mainfunction.cgi sub_1DA58 path traversal	A vulnerability has been found in DrayTek Vigor 2960 1.5.1.4 and classified as problematic. Affected by this vulnerability is the function sub_1DA58 of the file mainfunction.cgi. The manipulation leads to path traversal. This vulnerability is known as CVE-2023-1163. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-26111	nubosoftware node-static startsWith path traversal	A vulnerability which was classified as critical has been found in nubosoftware nodestatic. This issue affects the function startsWith. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-26111. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-1191	fastcms ZIP File TemplateController.java path traversal	A vulnerability classified as problematic has been found in fastcms. This affects an unknown part of the file admin /TemplateController.java of the component ZIP File Handler. The manipulation leads to path traversal. This vulnerability is uniquely identified as CVE-2023-1191. It is possible to initiate the attack remotely. Furthermore there is an exploit available. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	Protected by core rules	Detected by scanner as Local File Inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-33353	Wyomind Help Desk Extension up to 1.3.6 on Magento File Attachment Directory Setting path traversal (ID 50113 / EDB-50113)	A vulnerability was found in Wyomind Help Desk Extension up to 1.3.6. It has been declared as critical. This vulnerability affects unknown code of the component File Attachment Directory Setting. The manipulation leads to path traversal. This vulnerability was named CVE-2021-33353. The attack can only be done within the local network. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-26956	onekeyadmin 1.3.9 / admin1 /curd/code path traversal	A vulnerability has been found in onekeyadmin 1.3.9 and classified as problematic. This vulnerability affects unknown code of the file /admin1/curd/code. The manipulation leads to path traversal. This vulnerability was named CVE-2023-26956. The attack needs to be approached within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-26948	onekeyadmin 1.3.9 / admin1 /file/download path traversal	A vulnerability was found in onekeyadmin 1.3.9. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin1/file/download. The manipulation leads to path traversal. This vulnerability is handled as CVE-2023-26948. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-25814	metersphere up to 2.7.0 path traversal (GHSA-fwc3- 5h55-mh2j)	A vulnerability classified as critical was found in metersphere up to 2.7.0. This vulnerability affects unknown code. The manipulation leads to path traversal. This vulnerability was named CVE-2023-25814. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-25802	Hap-WI Roxy-WI prior 6.3.6.0 Web Interface path traversal (GHSA-qcmp-q5h3-784m)	A vulnerability was found in Hap-WI Roxy-WI. It has been rated as critical. This issue affects some unknown processing of the component Web Interface Handler. The manipulation leads to path traversal: &039;dir/../.. / filename&039;. The identification of this vulnerability is CVE-2023-25802. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-25803	Hap-WI Roxy-WI prior 6.3.5.0 Web Interface path traversal (GHSA-cv9w-j9gh- 5j3w)	A vulnerability classified as critical has been found in Hap- WI Roxy-WI. Affected is an unknown function of the component Web In-terface. The manipulation leads to path traversal. This vulnerability is traded as CVE-2023-25803. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-25804	Hap-WI Roxy-WI prior 6.3.5.0 Web Interface path traversal (GHSA-69j6-crq8- rrhv)	A vulnerability was found in Hap-WI Roxy-WI. It has been declared as critical. This vulnerability affects unknown code of the component Web Interface. The manipulation leads to path traversal: &039;.. / filedir&039;. This vulnerability was named CVE-2023-25804. The attack can be initiated remotely. There is no ex-ploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-25345	swig-templates/swig Tag path traversal (ID 88)	A vulnerability was found in swig-templates and swig and classified as problematic. This issue affects some unknown processing of the compo-nent Tag Handler. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-25345. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-0340	Custom Content Shortcode Plugin up to 4.0.2 on WordPress Shortcode Attribute path traversal	A vulnerability was found in Custom Content Short-code Plugin up to 4.0.2. It has been rated as critical. This issue affects some unknown processing of the component Shortcode Attribute Handler. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2023-0340. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2022-30037	XunRuiCMS up to 4.5.1 cron. php add file inclusion	A vulnerability was found in XunRuiCMS up to 4.5.1 and classified as critical. This issue affects the function add of the file cron.php. The manipula-tion leads to file inclusion. The identification of this vulnerability is CVE-2022-30037. The attack can only be done within the local network. There is no ex-ploit available.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2023-0467	WP Dark Mode Plugin up to 4.0.7 on Word-Press Shortcode style file inclusion	A vulnerability was found in WP Dark Mode Plugin up to 4.0.7. It has been declared as problematic. Affected by this vulnera-bility is an unknown func-tionality of the component Shortcode Handler. The manipulation of the ar-gument style leads to file inclusion. This vulnerability is known as CVE-2023-0467. The attack can only be done within the local network. There is no exploit avail-able. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Local File Inclusion attack.
CVE-2022-32199	ScriptCase up to 9.9.008 db_convert. php file path traversal	A vulnerability which was classified as problematic was found in ScriptCase up to 9.9.008. This affects an unknown part of the file db_convert.php. The ma-nipulation of the argument file leads to path traversal. This vulnerability is uniquely identified as CVE-2022- 32199. The attack needs to be approached within the local network. There is no exploit avail-able.	Protected by core rules	Detected by scanner as Local File Inclusion attack.

Malicious File Upload Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-45988	starsoftcomm Coo-Care 5.304 unre-stricted upload	A vulnerability which was classified as problematic was found in starsoft-comm CooCare 5.304. This affects an unknown part. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2022-45988. The attack needs to be approached locally. There is no exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-25402	CleverStupidDog yf-exam 1.8.0 unre-stricted upload	A vulnerability which was classified as critical was found in CleverStupidDog yfexam 1.8.0. Affected is an unknown function. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-25402. Ac-cess to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-24734	PMB 7.4.6 Image File camera_upload.php unrestricted upload	A vulnerability was found in PMB 7.4.6 and classi-fied as critical. This issue affects some unknown processing of the file camera_upload.php of the component Image File Handler. The manipulation leads to unrestricted upload. The identification of this vulnerability is CVE-2023-24734. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-26949	onekeyadmin 1.3.9 /admin1 /config/ update unrestricted upload	A vulnerability was found in onekeyadmin 1.3.9. It has been classified as critical. Affected is an unknown function of the file /admin1 /config/update. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-26949. Ac-cess to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2021-33352	Wyomind Help Desk Extension up to 1.3.6 on Magento Ticket Message unrestricted upload (ID 50113 / EDB-50113)	A vulnerability classified as problematic was found in Wyomind Help Desk Extension up to 1.3.6. This vulnerability affects unknown code of the com-ponent Ticket Message Handler. The manipula-tion leads to unrestricted upload. This vulnerability was named CVE-2021-33352. Access to the local network is required for this attack to succeed. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-24282	Poly Trio 8800 7.2.2.1094 Ringtone File unrestricted upload	A vulnerability classified as critical has been found in Poly Trio 8800 7.2.2.1094. This affects an unknown part of the component Ringtone File Handler. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-24282. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-27164	Halo up to 1.6.1 MD File unrestricted upload	A vulnerability classified as critical has been found in Halo up to 1.6.1. Affected is an unknown function of the component MD File Handler. The manipula-tion leads to unrestricted upload. This vulnerability is traded as CVE-2023-27164. Ac-cess to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1328	Guizhou 115cms 4.2 / admin /content/index unrestricted upload	A vulnerability was found in Guizhou 115cms 4.2. It has been classified as problematic. Affected is an unknown function of the file /admin/content/index. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-1328. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-1313	cockpit up to 2.4.0 unrestricted upload	A vulnerability classified as critical has been found in cockpit up to 2.4.0. This affects an unknown part. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-1313. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-23328	AvantFAX 3.3.7 FileUpload. php unrestricted upload	A vulnerability classified as critical was found in AvantFAX 3.3.7. Affected by this vulnerability is an unknown functionality of the file FileUpload.php. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-23328. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-0477	Auto Featured Image Plugin prior 3.9.16 on WordPress AJAX Endpoint unrestricted upload	A vulnerability which was classified as critical was found in Auto Featured Image Plugin. Affected is an unknown function of the component AJAX Endpoint. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-0477. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-1415	Simple Art Gallery 1.0 adminHome.php sliderPicSubmit unrestricted upload	A vulnerability was found in Simple Art Gallery 1.0. It has been declared as critical. This vulnerability affects the function sliderPicSubmit of the file adminHome.php. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-1415. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-27757	PerfreeBlog 3.1.1 JPG File /admin/user/uploadImg unrestricted upload (ID 13)	A vulnerability was found in PerfreeBlog 3.1.1. It has been declared as critical. This vulnerability affects unknown code of the file / admin/user /uploadImg of the component JPG File Handler. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-27757. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-27235	Jizhicms 2.4.5 phtml File CommonController.php unrestricted upload (ID 85)	A vulnerability was found in Jizhicms 2.4.5. It has been classified as critical. This affects an unknown part of the file \admin\c\ CommonController. php of the component phtml File Handler. The manipulation leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-27235. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-26262	Sitecore XP/XM 10.3 Language File unrestricted upload	A vulnerability which was classified as critical was found in Sitecore XP and XM 10.3. Affected is an unknown function of the component Language File Handler. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2023-26262. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-1433	SourceCodester Gadget Works Online Ordering System 1.0 Products controller. php filename unrestricted upload	A vulnerability was found in SourceCodester Gadget Works Online Ordering System 1.0. It has been classified as problematic. This affects an unknown part of the file admin/ products /controller. phpactionadd of the component Products Handler. The manipulation of the argument filename leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-1433. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-1442	Meizhou Qingyunke QYKCMS 4.3.0 Update /admin_system/api. php downurl unrestricted upload	A vulnerability was found in Meizhou Qingyunke QYKCMS 4.3.0. It has been classified as problematic. This affects an unknown part of the file /admin_ system/api. php of the component Update Handler. The manipulation of the argument downurl leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-1442. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-1479	SourceCodester Simple Music Player 1.0 save_music. php filename unrestricted upload	A vulnerability classified as critical has been found in SourceCodester Simple Music Player 1.0. Affected is an unknown function of the file save_music.php. The manipulation of the argument filename leads to unrestricted upload. This vulnerability is traded as CVE-2023-1479. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-1484	xzjie cms up to 1.0.3 / api /upload uploadFile unrestricted upload (I6INIT)	A vulnerability was found in xzjie cms up to 1.0.3 and classified as critical. This issue affects some unknown processing of the file /api /upload. The manipulation of the argument uploadFile leads to unrestricted upload. The identification of this vulnerability is CVE-2023-1484. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1501	RockOA 2.3.2 acloud-CosAction.php.SQL runAction fileid unrestricted upload	A vulnerability which was classified as critical was found in RockOA 2.3.2. This affects the function runAction of the file acloudCosAction. php. SQL. The manipulation of the argument fileid leads to unrestricted upload. This vulnerability is uniquely identified as CVE-2023-1501. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-1559	SourceCodester Storage Unit Rental Management System 1.0 classes/Users. php unrestricted upload	A vulnerability classified as problematic was found in SourceCodester Storage Unit Rental Management System 1.0. This vulnerability affects unknown code of the file classes/ Users.phpfsave. The manipulation leads to unrestricted upload. This vulnerability was named CVE-2023-1559. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2023-28725	General Bytes Crypto Application Server 20230120 Java Application deployments unrestricted upload (BATM-4780)	A vulnerability has been found in General Bytes Crypto Application Server 20230120 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /batm /app/admin/ standalone /deployments of the component Java Application Handler. The manipulation leads to unrestricted upload. This vulnerability is known as CVE-2023-28725. The attack can be launched remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as malicious file upload attack.
CVE-2020-19786	CSKaza CSZ CMS up to 1.2.2 PHP unrestricted upload (ID 20)	A vulnerability which was classified as critical was found in CSKaza CSZ CMS up to 1.2.2. Affected is an unknown function of the component PHP Handler. The manipulation leads to unrestricted upload. This vulnerability is traded as CVE-2020-19786. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as malicious file upload attack.

SQL Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-23315	PrestaShop up to 4.5.5 initContent sql injection	A vulnerability which was classified as critical was found in PrestaShop up to 4.5.5. This affects the function stripejsValidationModuleFrontController:: initContent. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-23315. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1151	SourceCodester Electronic Medical Records System	A vulnerability was found in SourceCodester Electronic Medical Records System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file administrator.php of the component Cookie Handler. The manipulation of the argument userid leads to sql injection. This vulnerability is known as CVE-2023-1151. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-26780	CleverStupidDog yf-exam 1.8.0 sql injection	A vulnerability classified as critical has been found in CleverStupidDog yf-exam 1.8.0. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-26780. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1165	Zhong Bang CRMEB Java 1.3.4 list keywords sql injection (ID 10)	A vulnerability was found in Zhong Bang CRMEB Java 1.3.4. It has been classified as critical. This affects an unknown part of the file /api/admin/system/store/order/list. The manipulation of the argument keywords leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1165. The attack needs to be initiated within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24641	SourceCodester Judging Management System 1.0 /phpjms/updateview.php sid sql injection	A vulnerability has been found in SourceCodester Judging Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /php-jms/updateview.php. The manipulation of the argument sid leads to sql injection. This vulnerability is known as CVE-2023- 24641. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24642	SourceCodester Judging Management System 1.0 updateTxtview.php sid sql injection	A vulnerability was found in SourceCodester Judging Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /php-jms /updateTxtview.php. The manipulation of the argument sid leads to sql injection. This vulnerability is handled as CVE-2023-24642. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-24643	SourceCodester Judging Management System 1.0 updateBlankTxtview.php sid sql injection	A vulnerability was found in SourceCodester Judging Management System 1.0. It has been classified as critical. This affects an unknown part of the file /php-jms/updateBlankTxtview. php. The manipulation of the argument sid leads to sql injection. This vulnerability is uniquely identified as CVE-2023-24643. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-0631	Paid Memberships Pro Plugin up to 2.9.11 on WordPress Shortcode sql injection	A vulnerability was found in Paid Memberships Pro Plugin up to 2.9.11. It has been classified as critical. This affects an unknown part of the component Shortcode Handler. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-0631. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1253	SourceCodester Health Center Patient Record Management System 1.0 login.php username sql injection	A vulnerability which was classified as critical was found in SourceCodester Health Center Patient Record Management System 1.0. This affects an unknown part of the file login.php. The manipulation of the argument username leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1253. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24763	Xen Forum up to 2.13.0 on PrestaShop sql injection	A vulnerability was found in Xen Forum up to 2.13.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-24763. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24781	Funadmin 3.2.0 \member\MemberLevel.php selectFields sql injection	A vulnerability classified as critical has been found in Funadmin 3.2.0. This affects an unknown part of the file \member\MemberLevel. php. The manipulation of the argument selectFields leads to sql injection. This vulnerability is uniquely identified as CVE-2023-24781. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24789	jeecg-boot 3.4.4 Building Block Report sql injection (ID 4511)	A vulnerability which was classified as critical was found in jeecg-boot 3.4.4. Affected is an unknown function of the component Building Block Report. The manipulation leads to sql injection. This vulnerability is traded as CVE-2023- 24789. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1211	phpipam up to 1.5.1 sql injection	A vulnerability has been found in phpipam up to 1.5.1 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-1211. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1276	SUL1SS_shop Order.php keyword sql injection	A vulnerability which was classified as critical has been found in SUL1SS_shop. This issue affects some unknown processing of the file application\merch\controller\Order.php. The manipulation of the argument keyword leads to sql injection. The identification of this vulnerability is CVE- 2023-1276. The attack may be initiated remotely. Furthermore there is an exploit available. This product does not use versioning. This is why information about affected and unaffected releases are unavailable.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-25223	CRMEB Java up to 1.3.4 /api /admin/user/list sql injection	A vulnerability was found in CRMEB Java up to 1.3.4. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /api/admin/user/list. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-25223. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24780	Funadmin 3.2.0 / databases /table/columns id sql injection	A vulnerability was found in Funadmin 3.2.0. It has been classified as critical. Affected is an unknown function of the file / databases/table /columns. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-24780. The attack needs to be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-26922	Varisicte matrix-gui 2.0 matrixgui-2.0 shell_exect sql injection	A vulnerability was found in Varisicte matrix-gui 2.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file \www\pages\matrix-gui-2.0. The manipulation of the argument shell_exect leads to sql injection. This vulnerability is known as CVE-2023-26922. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24773	Funadmin 3.2.0 /databases /database/list id sql injection	A vulnerability was found in Funadmin 3.2.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /databases/database/list. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-24773. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24775	Funadmin 3.2.0 \member\Member.php selectFields sql injection	A vulnerability which was classified as critical was found in Funadmin 3.2.0. This affects an unknown part of the file \member\Member.php. The manipulation of the argument selectFields leads to sql injection. This vulnerability is uniquely identified as CVE-2023-24775. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-27207	SourceCodester Online Pizza Ordering System 1.0 /admin / manage_user.php id sql injection	A vulnerability which was classified as critical has been found in Source-Codester Online Pizza Ordering System 1.0. This issue affects some un-known processing of the file /admin /manage_user. php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-27207. The attack may be initiated remotely. There is no exploit avail-able.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-27210	SourceCodester Online Pizza Ordering System 1.0 /admin / view_order.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Online Pizza Ordering System 1.0. Affected is an unknown function of the file /admin/view_order. php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-27210. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-27204	SourceCodester Best POS Management System 1.0 /kruxton/ manage_user.php id sql injection	A vulnerability classified as critical has been found in SourceCodester Best POS Management System 1.0. This affects an unknown part of the file /krux-ton/manage_user. php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-27204. It is possible to initiate the attack re-motely. There is no exploit	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-27214	SourceCodester On-line Student Manage-ment System 1.0 be-tween-date-reprts-details. php fromdate/todate sql injection	A vulnerability was found in SourceCodester Online Student Management System 1.0 and classi-fied as critical. This issue affects some unknown processing of the file / eduauth/student /be-tween-date-reprtsdetails. php. The manipulation of the argument fromdate/ todate leads to sql injec-tion. The identification of this vulnerability is CVE- 2023-27214. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1291	SourceCodester Sales Tracker Man-agement System 1.0 manage_client.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Sales Tracker Management System 1.0. This affects an unknown part of the file admin/clients /manage_ client.php. The manipu-lation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1291. It is possible to initiate the attack remote-ly. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-27202	SourceCodester Best POS Management System 1.0 /kruxton/ receipt.php id sql injection	A vulnerability was found in SourceCodester Best POS Management System 1.0. It has been declared as critical. Affected by this vulnerability is an un-known functionality of the file /kruxton/receipt.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023- 27202. The attack can be launched re-motely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1290	SourceCodester Sales Tracker Management System 1.0 view_client.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Sales Tracker Management System 1.0. Affected by this issue is some unknown functionality of the file admin/clients/view_client.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-1290. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1294	SourceCodester File Tracker Manager System 1.0 POST Parameter /file_manager/login. php username sql injection	A vulnerability was found in SourceCodester File Tracker Manager System 1.0. It has been classified as critical. Affected is an unknown function of the file /file_manager/login. php of the component POST Parameter Handler. The manipulation of the argument username leads to sql injection. This vulnerability is traded as CVE-2023-1294. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-27203	SourceCodester Best POS Management System 1.0 /billing /home.php id sql injection	A vulnerability was found in SourceCodester Best POS Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file / billing /home.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-27203. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1292	SourceCodester Sales Tracker Management System 1.0 classes/Master.php delete_client id sql injection	A vulnerability has been found in SourceCodester Sales Tracker Management System 1.0 and classified as critical. This vulnerability affects the function delete_client of the file classes/Master.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-1292. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-27205	SourceCodester Best POS Management System 1.0 sales_report.php month sql injection	A vulnerability classified as critical was found in SourceCodester Best POS Management System 1.0. This vulnerability affects unknown code of the file / kruxton/sales_report.php. The manipulation of the argument month leads to sql injection. This vulnerability was named CVE-2023-27205. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24777	Funadmin 3.2.0 / databases /table/list id sql injection	A vulnerability was found in Funadmin 3.2.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /databases/table/list. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-24777. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1301	SourceCodester Friendly Island Pizza Website and Ordering System 1.0 GET Parameter deleteorder.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. Affected by this issue is some unknown functionality of the file deleteorder.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-1301. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-27213	SourceCodester Online Student Management System 1.0 search.php searchdata sql injection	A vulnerability has been found in SourceCodester Online Student Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /eduauth/student/search.php. The manipulation of the argument searchdata leads to sql injection. This vulnerability is known as CVE-2023- 27213. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1300	SourceCodester COVID 19 Testing Management System 1.0 POST Parameter patientreport.php searchdata sql injection	A vulnerability classified as critical was found in SourceCodester COVID 19 Testing Management System 1.0. Affected by this vulnerability is an unknown functionality of the file patient-report.php of the component POST Parameter Handler. The manipulation of the argument searchdata leads to sql injection. This vulnerability is known as CVE-2023-1300. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24782	Funadmin 3.2.0 / databases /database/edit id sql injection	A vulnerability was found in Funadmin 3.2.0. It has been classified as critical. Affected is an unknown function of the file / databases /database/edit. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-24782. The attack can only be initiated withinthe local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1311	SourceCodester Friendly Island Pizza Website and Ordering System 1.0 GET Parameter large.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. This affects an unknown part of the file large.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1311. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1308	SourceCodester Online Graduate Tracer System 1.0 admin/adminlog.php user sql injection	A vulnerability classified as critical has been found in SourceCodester Online Graduate Tracer System 1.0. Affected is an unknown function of the file admin/adminlog.php. The manipulation of the argument user leads to sql injection. This vulnerability is traded as CVE-2023-1308. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-24774	Funadmin 3.2.0 Auth.php selectFields sql injection (ID 12)	A vulnerability was found in Funadmin 3.2.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file \controller\auth\Auth.php. The manipulation of the argument selectFields leads to sql injection. This vulnerability is known as CVE-2023-24774. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1309	SourceCodester Online Graduate Tracer System 1.0 admin/search_it.php input sql injection	A vulnerability classified as critical was found in SourceCodester Online Graduate Tracer System 1.0. Affected by this vulnerability is an unknown functionality of the file admin /search_it.php. The manipulation of the argument input leads to sql injection. This vulnerability is known as CVE-2023-1309. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1310	SourceCodester Online Graduate Tracer System 1.0 admin/prof.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester Online Graduate Tracer System 1.0. Affected by this issue is some unknown functionality of the file admin/prof.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-1310. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1351	SourceCodester Computer Parts Sales and Inventory System 1.0 cust_transac.php phonenumber sql injection	A vulnerability classified as critical has been found in SourceCodester Computer Parts Sales and Inventory System 1.0. This affects an unknown part of the file cust_transac.php. The manipulation of the argument phonenumber leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1351. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1352	SourceCodester Design and Implementation of Covid-19 Directory on Vaccination System / admin/login.php sql injection	A vulnerability which was classified as critical has been found in SourceCodester Design and Implementation of Covid-19 Directory on Vaccination System 1.0. This issue affects some unknown processing of the file / admin /login.php. The manipulation of the argument txtusername/txtpassword leads to sql injection. The identification of this vulnerability is CVE- 2023-1352. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1360	SourceCodester Employee Payslip Generator with Sending Mail 1.2.0 New User Creation classes/Users.php username sql injection	A vulnerability was found in SourceCodester Employee Payslip Generator with Sending Mail 1.2.0 and classified as critical. This issue affects some unknown processing of the file classes/Users.phpfsave of the component New User Creation. The manipulation of the argument username leads to sql injection. The identification of this vulnerability is CVE-2023-1360. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1358	SourceCodester Gadget Works Online Ordering System 1.0 POST Parameter login.php user_email sql injection	A vulnerability which was classified as critical was found in SourceCodester Gadget Works Online Ordering System 1.0. This affects an unknown part of the file /philosophy/admin /login.php of the component POST Parameter Handler. The manipulation of the argument user_ email leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1358. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1361	unilogies bumsys up to 2.0.1 sql injection	A vulnerability classified as critical was found in unilogies bumsys up to 2.0.1. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2023-1361. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-0037	10Web Map Builder for Google Maps Plugin prior 1.0.73 on WordPress sql injection	A vulnerability which was classified as critical has been found in 10Web Map Builder for Google Maps Plugin. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-0037. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1364	SourceCodester Online Pizza Ordering System 1.0 GET Parameter category. php id sql injection	A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file category.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-1364. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1368	XHCMS 1.0 POST Parameter login.php user sql injection	A vulnerability was found in XHCMS 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login.php of the component POST Parameter Handler. The manipulation of the argument user leads to sql injection. This vulnerability was named CVE-2023-1368. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1366	SourceCodester Yoga Class Registration System 1.0 manage_ category.php query id sql injection	A vulnerability was found in SourceCodester Yoga Class Registration System 1.0. It has been classified as critical. This affects the function query of the file admin/categories / manage_category.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1366. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1365	SourceCodester Online Pizza Ordering System 1.0 /admin / ajax.php username sql injection	A vulnerability was found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin /ajax.php. The manipulation of the argument username leads to sql injection. This vulnerability is handled as CVE-2023-1365. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1378	SourceCodester Friendly Island Pizza Website and Ordering System 1.0 POST Parameter paypal-success.php cusid sql injection	A vulnerability classified as critical was found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. This vulnerability affects unknown code of the file paypalsuccess. php of the component POST Parameter Handler. The manipulation of the argument cusid leads to sql injection. This vulnerability was named CVE-2023-1378. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-25206	ws_productreviews up to 3.6.1 on PrestaShop sql injection	A vulnerability classified as critical was found in ws_productreviews up to 3.6.1. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2023-25206. Access to the local network is required for this attack. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-25207	dpdfrance up to 6.1.2 on PrestaShop dpdfrance/ajax.php sql injection	A vulnerability which was classified as critical was found in dpdfrance up to 6.1.2. This affects an unknown part of the file dpdfrance/ajax.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-25207. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-27052	Moosikay E-Commerce System 1.0 / admin/delete_user.php id sql injection	A vulnerability was found in Moosikay ECommerce System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file / admin/delete_user.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-27052. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1407	SourceCodester Student Study Center Desk Management System 1.0 manage_user.php id sql injection	A vulnerability classified as critical was found in SourceCodester Student Study Center Desk Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/user/manage_user.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-1407. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1416	Simple Art Gallery 1.0 adminHome.php social_facebook sql injection	A vulnerability classified as critical has been found in Simple Art Gallery 1.0. Affected is an unknown function of the file adminHome.php. The manipulation of the argument social_facebook leads to sql injection. This vulnerability is traded as CVE-2023-1416. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24732	SourceCodester Simple Customer Relationship Management System 1.0 User Profile Update gender sql injection	A vulnerability was found in SourceCodester Simple Customer Relationship Management System 1.0. It has been classified as critical. This affects an unknown part of the component User Profile Update Handler. The manipulation of the argument gender leads to sql injection. This vulnerability is uniquely identified as CVE-2023-24732. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24726	PHPGurukul Art Gallery Management System 1.0 Enquiry Page viewid sql injection	A vulnerability which was classified as critical has been found in PHPGurukul Art Gallery Management System 1.0. This issue affects some unknown processing of the component Enquiry Page. The manipulation of the argument viewid leads to sql injection. The identification of this vulnerability is CVE- 2023-24726. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24728	SourceCodester Simple Customer Relationship Management System 1.0 User Profile Update contact sql injection	A vulnerability classified as critical was found in SourceCodester Simple Customer Relationship Management System 1.0. This vulnerability affects unknown code of the component User Profile Update Handler. The manipulation of the argument contact leads to sql injection. This vulnerability was named CVE-2023-24728. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24730	SourceCodester Simple Customer Relationship Management System 1.0 User Profile Update company sql injection	A vulnerability has been found in SourceCodester Simple Customer Relationship Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the component User Profile Update Handler. The manipulation of the argument company leads to sql injection. This vulnerability is known as CVE-2023-24730. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-24729	SourceCodester Simple Customer Relationship Management System 1.0 User Profile Update address sql injection	A vulnerability which was classified as critical was found in SourceCodester Simple Customer Relationship Management System 1.0. Affected is an unknown function of the component User Profile Update Handler. The manipulation of the argument address leads to sql injection. This vulnerability is traded as CVE-2023-24729. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-24731	SourceCodester Simple Customer Relationship Management System 1.0 User Profile Update query sql injection	A vulnerability was found in SourceCodester Simple Customer Relationship Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the component User Profile Update Handler. The manipulation of the argument query leads to sql injection. This vulnerability is handled as CVE-2023-24731. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-1379	SourceCodester Friendly Island Pizza Website and Ordering System 1.0 POST Parameter addmem.php firstname sql injection	A vulnerability was found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. It has been rated as critical. This issue affects some unknown processing of the file addmem.php of the component POST Parameter Handler. The manipulation of the argument firstname leads to sql injection. The identification of this vulnerability is CVE-2023-1379. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-27709	DedeCMS 5.7.106 dedestory_catalog.php rank_* sql injection	A vulnerability classified as critical has been found in DedeCMS 5.7.106. This affects an unknown part of the file dedestory_catalog.php. The manipulation of the argument rank_ leads to sql injection. This vulnerability is uniquely identified as CVE-2023-27709. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-27041	School Registration and Fee System 1.0 edit_user.php id sql injection	A vulnerability which was classified as critical was found in School Registration and Fee System 1.0. This affects an unknown part of the file edit_user.php. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2023-27041. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.
CVE-2023-27707	DedeCMS 5.7.106 / dede /group_store.php rank_* sql injection	A vulnerability was found in DedeCMS 5.7.106. It has been rated as critical. Affected by this issue is some unknown functionality of the file /dede/group_store.php. The manipulation of the argument rank_ leads to sql injection. This vulnerability is handled as CVE-2023-27707. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL Injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-27250	Online Book Store Project 1.0 bookPer-Pub.php sql injection	A vulnerability was found in Online Book Store Project 1.0. It has been rated as critical. This issue affects some un-known processing of the file /bookstore/bookPer-Pub.php. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2023-27250. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1439	SourceCodester Med-icine Tracker System 1.0 GET Parameter view_details.php sql injection	A vulnerability which was classified as critical has been found in Source-Codester Medicine Tracker System 1.0. This issue affects some unknown processing of the file med-icines /view_details.php of the component GET Parameter Handler. The manipulation of the ar-gument GET leads to sql injection. The identification of this vulnerability is CVE-2023-1439. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1441	SourceCodester Automatic Question Paper Generator Sys-tem 1.0 GET Parame-ter view_course.php id sql injection	A vulnerability has been found in SourceCodester Automatic Question Paper Generator System 1.0 and classified as critical. Af-fected by this vulnerability is an unknown function-ality of the file admin/courses /view_course.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-1441. The attack can be launched re-motely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1440	SourceCodester Automatic Question Paper Generator Sys-tem 1.0 GET Parame-ter manage_user.php id sql injection	A vulnerability which was classified as critical was found in SourceCodester Automatic Question Paper Generator System 1.0. Affected is an unknown function of the file users /user/manage_user.php of the component GET Pa-rameter Handler. The ma-nipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-1440. It is possible to launch the attack remotely. Further-more there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1474	SourceCodester Automatic Question Paper Generator Sys-tem 1.0 GET Param-eter manage_ques-tion_paper.php id sql injection	A vulnerability classified as critical was found in SourceCodester Auto-matic Question Paper Generator System 1.0. This vulnerability affects unknown code of the file users/question_papers / manage_question_paper.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-1474. The attack can be initiated remotely. Furthermore there is an exploit avail-able.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1454	jeecg-boot 3.5.0 jmreport /qurestSql apiSelectId sql injection	A vulnerability classified as critical has been found in jeecg-boot 3.5.0. This affects an unknown part of the file jmreport/qurestSql. The manipulation of the argument apiSelectId leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1454. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1461	SourceCodester Canteen Management System 1.0 createCategories.php query categoriesStatus sql injection	A vulnerability was found in SourceCodester Canteen Management System 1.0. It has been declared as critical. This vulnerability affects the function query of the file createCategories. php. The manipulation of the argument categoriesStatus leads to sql injection. This vulnerability was named CVE-2023-1461. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1459	SourceCodester Canteen Management System 1.0 changeUsername. php username sql injection	A vulnerability was found in SourceCodester Canteen Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file changeUsername.php. The manipulation of the argument username leads to sql injection. This vulnerability is handled as CVE-2023-1459. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1475	SourceCodester Canteen Management System 1.0 createuser.php query uemail sql injection	A vulnerability which was classified as critical has been found in SourceCodester Canteen Management System 1.0. This issue affects the function query of the file createuser.php. The manipulation of the argument uemail leads to sql injection. The identification of this vulnerability is CVE-2023-1475. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1494	IBOS 4.5.5 ApiController.php emailids sql injection	A vulnerability classified as critical has been found in IBOS 4.5.5. Affected is an unknown function of the file ApiController.php. The manipulation of the argument emailids leads to sql injection. This vulnerability is traded as CVE-2023-1494. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1483	XiaoBingBy TeaCMS up to 2.0.2 /admin/getallarticleinfo searchInfo sql injection	A vulnerability has been found in XiaoBingBy TeaCMS up to 2.0.2 and classified as critical. This vulnerability affects unknown code of the file /admin/getallarticleinfo. The manipulation of the argument searchInfo leads to sql injection. This vulnerability was named CVE-2023-1483. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1480	SourceCodester Monitoring of Students Cyber Accounts System 1.0 POST Parameter login.php un sql injection	A vulnerability classified as critical was found in SourceCodester Monitoring of Students Cyber Accounts System 1.0. Affected by this vulnerability is an unknown functionality of the file login.php of the component POST Parameter Handler. The manipulation of the argument un leads to sql injection. This vulnerability is known as CVE-2023-1480. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1495	Rebuild up to 3.2.3 list queryListOfConfig q sql injection (ID 594)	A vulnerability classified as critical was found in Rebuild up to 3.2.3. Affected by this vulnerability is the function queryListOfConfig of the file /admin/robot/approval/list. The manipulation of the argument q leads to sql injection. This vulnerability is known as CVE-2023-1495. The attack can be launched remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1499	code-projects Simple Art Gallery 1.0 adminHome.php reach_city sql injection	A vulnerability classified as critical was found in code-projects Simple Art Gallery 1.0. Affected by this vulnerability is an unknown functionality of the file adminHome.php. The manipulation of the argument reach_city leads to sql injection. This vulnerability is known as CVE-2023-1499. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-26905	Alphaware Simple ECommerce System 1.0 /alphaware/details.php id sql injection	A vulnerability was found in Alphaware Simple E-Commerce System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /alphaware/details.php. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-26905. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1502	SourceCodester Alphaware Simple E-Commerce System 1.0 edit_customer.php firstname /mi/lastname sql injection	A vulnerability was found in SourceCodester Alphaware Simple E-Commerce System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file function/edit_customer.php. The manipulation of the argument firstname/mi/lastname with the input a&039; RLIKE SLEEP AND &039; dAbu&039;&039;dAbu leads to sql injection. This vulnerability is handled as CVE-2023-1502. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1504	SourceCodester Alphaware Simple E-Commerce System 1.0 email/password sql injection	A vulnerability classified as critical was found in SourceCodester Alphaware Simple ECommerce System 1.0. This vulnerability affects unknown code. The manipulation of the argument email/password with the input test1%40test.com &039; AND))dltn) AND &039; PhRa&039;&039;PhRa leads to sql injection. This vulnerability was named CVE-2023-1504. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-0875	WP Meta SEO Plugin up to 4.5.2 on WordPress sql injection	A vulnerability which was classified as critical has been found in WP Meta SEO Plugin up to 4.5.2. Affected by this issue is some unknown functionality. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-0875. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1503	SourceCodester Alphaware Simple E-Commerce System 1.0 admin/admin_index.php username/password sql injection	A vulnerability classified as critical has been found in SourceCodester Alphaware Simple ECommerce System 1.0. This affects an unknown part of the file admin/admin_index.php. The manipulation of the argument username/password with the input admin&039; AND)) meUD)-- hLiX leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1503. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1505	SourceCodester E-Commerce System 1.0 setDiscount.php id sql injection	A vulnerability which was classified as critical has been found in SourceCodester ECommerce System 1.0. This issue affects some unknown processing of the file /ecommerce/admin/settings/setDiscount.php. The manipulation of the argument id with the input 201737 AND))0oAD) leads to sql injection. The identification of this vulnerability is CVE-2023-1505. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1545	nilsteampassnet teampass prior 3.0.0.23 sql injection	A vulnerability was found in nilsteampassnet teampass. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-1545. The attack can only be initiated within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1556	SourceCodester Judging Management System 1.0 summary_results.php main_event_id sql injection	A vulnerability was found in SourceCodester Judging Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file summary_results.php. The manipulation of the argument main_event_id leads to sql injection. This vulnerability is known as CVE-2023-1556. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1578	pimcore up to 10.5.18 sql injection	A vulnerability classified as critical has been found in pimcore up to 10.5.18. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1578. Local access is required to approach this attack. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1571	DataGear up to 4.5.0 pagingQueryData queryOrder sql injection	A vulnerability which was classified as critical was found in DataGear up to 4.5.0. This affects an unknown part of the file /analysisProject /pagingQueryData. The manipulation of the argument queryOrder leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1571. It is possible to initiate the attack remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1563	SourceCodester Student Study Center Desk Management System 1.0 /admin/assign /assign.php id sql injection	A vulnerability has been found in SourceCodester Student Study Center Desk Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/assign /assign.php. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2023-1563. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1566	SourceCodester Medical Certificate Generator App 1.0 action.php id sql injection	A vulnerability was found in SourceCodester Medical Certificate Generator App 1.0. It has been declared as critical. This vulnerability affects unknown code of the file action.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-1566. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-27569	eo_tags Package up to 1.2.x on PrestaShop Header Referer sql injection	A vulnerability classified as critical has been found in eo_tags Package up to 1.2.x. This affects an unknown part of the component Header Handler. The manipulation of the argument Referer leads to sql injection. This vulnerability is uniquely identified as CVE-2023-27569. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1564	SourceCodester Air Cargo Management System 1.0 GET Parameter update_status.php id sql injection	A vulnerability was found in SourceCodester Air Cargo Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file admin/transactions/update_status.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. This vulnerability is handled as CVE-2023-1564. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-27638	tshirtecommerce 2.1.4 on PrestaShop GET Parameter hookActionCartSave /updateCustomizationTable tshirtecommerce_design_cart_id sql injection	A vulnerability was found in tshirtecommerce 2.1.4. It has been rated as critical. Affected by this issue is the function hookActionCartSave /updateCustomizationTable of the component GET Parameter Handler. The manipulation of the argument tshirtecommerce_design_cart_id leads to sql injection. This vulnerability is handled as CVE-2023-27638. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-27637	tshirtecommerce 2.1.4 on PrestaShop designer.php GET sql injection	A vulnerability was found in tshirtecommerce 2.1.4 and classified as critical. This issue affects some unknown processing of the file designer.php. The manipulation of the argument GET leads to sql injection. The identification of this vulnerability is CVE-2023-27637. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1594	novel-plus 3.6.2 sys/menu/list MenuService sort sql injection	A vulnerability which was classified as critical was found in novel-plus 3.6.2. Affected is the function MenuService of the file sys/menu/list. The manipulation of the argument sort leads to sql injection. This vulnerability is traded as CVE-2023-1594. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1595	novel-plus 3.6.2 common/log /list sort sql injection	A vulnerability has been found in novel-plus 3.6.2 and classified as critical. Affected by this vulnerability is an unknown functionality of the file common/log/list. The manipulation of the argument sort leads to sql injection. This vulnerability is known as CVE-2023-1595. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-28660	Events Made Easy Plugin up to 2.3.14 on WordPress eme_re-currences_list search_name sql injection	A vulnerability classified as critical was found in Events Made Easy Plugin up to 2.3.14. This vulnera-bility affects the function eme_recurrences_list. The manipulation of the argument search_name leads to sql injection. This vulnerability was named CVE-2023-28660. The attack can be initiated remotely. There is no ex-ploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-28659	Waiting One-click Countdowns Plugin up to 0.6.2 on WordPress pbc_save_downs pbc_down[meta][id] sql injection	A vulnerability was found in Waiting One-click Countdowns Plugin up to 0.6.2. It has been declared as critical. Affected by this vulnerability is the func-tion pbc_save_downs. The manipulation of the argument pbc_down [meta][id] leads to sql injection. This vulnerability is known as CVE-2023-28659. The attack can be launched re-motely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-28661	WP Popup Banners Plugin up to 1.2.5 on WordPress get_pop-up_data value sql injection	A vulnerability which was classified as critical has been found in WP Popup Banners Plugin up to 1.2.5. This issue affects the function get_popup_data. The manipulation of the argument value leads to sql injection. The identification of this vulnerability is CVE-2023-28661. The attack may be initiated remotely. There is no exploit avail-able.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-28663	Formidable PRO2PDF Plugin up to 3.10 on WordPress fpropdf_ export_file fieldmap sql injection	A vulnerability which was classified as critical was found in Formidable PRO2PDF Plugin up to 3.10. Affected is the function fpropdf_ex-port_file. The manipulation of the argument fieldmap leads to sql injection. This vulnerability is traded as CVE-2023-28663. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1590	SourceCodester Online Tours & Travels Management System 1.0 currency.php exec id sql injection	A vulnerability was found in SourceCodester Online Tours & Travels Manage-ment System 1.0 and classified as critical. This issue affects the function exec of the file admin/ operations /currency.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2023-1590. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1589	SourceCodester Online Tours & Travels Management System 1.0 approve_de-lete.php exec id sql injection	A vulnerability has been found in SourceCodester Online Tours & Travels Management System 1.0 and classified as critical. This vulnerability affects the function exec of the file admin/operations / approve_delete.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2023-1589. The attack can be initiated remotely. Furthermore there is an exploit avail-able.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-24655	Simple Customer Relationship Management System 1.0 Profile Update name sql injection	A vulnerability was found in Simple Customer Relationship Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the component Profile Update Handler. The manipulation of the argument name leads to sql injection. This vulnerability is handled as CVE-2023-24655. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1606	novel-plus 3.6.2 DictController. java orderby sql injection	A vulnerability was found in novel-plus 3.6.2 and classified as critical. Affected by this issue is some unknown functionality of the file DictController.java. The manipulation of the argument orderby leads to sql injection. This vulnerability is handled as CVE-2023-1606. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1610	Rebuild up to 3.2.3 / project /tasks/list sql injection (ID 597)	A vulnerability which was classified as critical has been found in Rebuild up to 3.2.3. Affected by this issue is some unknown functionality of the file / project/tasks/list. The manipulation leads to sql injection. This vulnerability is handled as CVE-2023-1610. The attack may be launched remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-28662	Gift Cards Plugin up to 4.3.1 on WordPress wpgv_doajax_voucher_pdf_save_func template sql injection	A vulnerability was found in Gift Cards Plugin up to 4.3.1. It has been rated as critical. Affected by this issue is the function wpgv_doajax_voucher_pdf_save_func. The manipulation of the argument template leads to sql injection. This vulnerability is handled as CVE-2023-28662. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1612	Rebuild up to 3.2.3 /files/list-file sql injection	A vulnerability which was classified as critical was found in Rebuild up to 3.2.3. This affects an unknown part of the file / files/list-file. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1612. It is possible to initiate the attack remotely. Furthermore there is an exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1607	novel-plus 3.6.2 / common /sysFile/list sort sql injection	A vulnerability was found in novel-plus 3.6.2. It has been classified as critical. This affects an unknown part of the file / common/sysFile/list. The manipulation of the argument sort leads to sql injection. This vulnerability is uniquely identified as CVE-2023-1607. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1608	Zhong Bang CRMEB Java up to 1.3.4 list getAdminList cateId sql injection (ID 11)	A vulnerability was found in Zhong Bang CRMEB Java up to 1.3.4. It has been declared as critical. This vulnerability affects the function getAdmin-List of the file /api/admin/store/product /list. The manipulation of the argument cateId leads to sql injection. This vulnerability was named CVE-2023-1608. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-24787	ChurchCRM 4.5.3 EventAttendance.php Event sql injection	A vulnerability was found in ChurchCRM 4.5.3. It has been rated as critical. This issue affects some unknown processing of the file /churchcrm/EventAttendance.php. The manipulation of the argument Event leads to sql injection. The identification of this vulnerability is CVE-2023-24787. The attack can only be initiated within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-24788	NotrinosERP 0.7 customer_delivery.php OrderNumber sql injection	A vulnerability was found in NotrinosERP 0.7. It has been declared as critical. This vulnerability affects unknown code of the file /NotrinosERP /sales/customer_delivery.php. The manipulation of the argument OrderNumber leads to sql injection. This vulnerability was named CVE-2023-24788. The attack can only be done within the local network. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-27847	xipblog up to 2.0.1 on PrestaShop xipcategoryclass /xipposts-class sql injection	A vulnerability has been found in xipblog up to 2.0.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the component xipcategoryclass/xippostsclass. The manipulation leads to sql injection. This vulnerability is known as CVE-2023-27847. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-26959	PHPGurukul Park Ticketing Management System 1.0 User Name sql injection	A vulnerability has been found in PHPGurukul Park Ticketing Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality. The manipulation of the argument User Name leads to sql injection. This vulnerability is known as CVE-2023-26959. The attack needs to be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-0955	WP Statistics Plugin up to 13.x on WordPress sql injection	A vulnerability classified as critical has been found in WP Statistics Plugin up to 13.x. This affects an unknown part. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2023-0955. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1770	SourceCodester Grade Point Average GPA Calculator 1.0 Master.php get_scale perc sql injection	A vulnerability has been found in SourceCodester Grade Point Average GPA Calculator 1.0 and classified as critical. Affected by this vulnerability is the function get_scale of the file Master.php. The manipulation of the argument perc leads to sql injection. This vulnerability is known as CVE-2023-1770. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.
CVE-2023-1785	SourceCodester Earnings and Expense Tracker App 1.0 manage_user.php id sql injection	A vulnerability was found in SourceCodester Earnings and Expense Tracker App 1.0. It has been classified as critical. Affected is an unknown function of the file manage_user.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2023-1785. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack.

Cross-Site Scripting Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1104	FlatPress up to 1.2 cross-site scripting	A vulnerability was found in FlatPress up to 1.2. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1104. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1117	pimcore up to 10.5.17 cross-site scripting	A vulnerability was found in pimcore up to 10.5.17. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023- 1117. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1116	pimcore up to 10.5.17 cross-site scripting	A vulnerability was found in pimcore up to 10.5.17. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1116. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1115	pimcore up to 10.5.17 cross-site scripting	A vulnerability was found in pimcore up to 10.5.17 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-1115. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1113	SourceCodester Simple Payroll System 1.0 POST Parameter admin/ fullname cross-site scripting	A vulnerability was found in SourceCodester Simple Payroll System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file admin/pageadmin of the component POST Parameter Handler. The manipulation of the argument fullname leads to cross-site scripting. This vulnerability is known as CVE-2023-1113. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-26608	VXControl SOLDR 1.1.0 Module Editor cross-site scripting (ID 89)	A vulnerability was found in VXControl SOLDR 1.1.0 and classified as problematic. Affected by this issue is some unknown functionality of the component Module Editor. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-26608. The attack may be launched remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack.
CVE-2023-1147	flatpress up to 1.2 cross-site scripting	A vulnerability classified as problematic was found in flatpress up to 1.2. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023- 1147. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1146	flatpress up to 1.2 cross-site scripting	A vulnerability classified as problematic has been found in flatpress up to 1.2. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1146. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1148	flatpress up to 1.2 cross-site scripting	A vulnerability which was classified as problematic has been found in flatpress up to 1.2. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-1148. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1025	Simple File List Plugin up to 6.0.9 on WordPress cross-site scripting	A vulnerability was found in Simple File List Plugin up to 6.0.9 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-1025. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1156	SourceCodester Health Center Patient Record Management System 1.0 admin /fecalysis_form. php itr_no crosssite scripting	A vulnerability classified as problematic was found in SourceCodester Health Center Patient Record Management System 1.0. This vulnerability affects unknown code of the file admin /fecalysis_form. php. The manipulation of the argument itr_no leads to cross-site scripting. This vulnerability was named CVE-2023-1156. The attack can be initiated remotely. Furthermore there is an exploit avail- able.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0175	Smart Logo Show- case Lite Plugin up to 1.1.9 on WordPress Shortcode cross-site scripting	A vulnerability which was classified as problematic has been found in Smart Logo Showcase Lite Plugin up to 1.1.9. This issue af- fects some unknown pro- cessing of the component Shortcode Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023- 0175. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0365	React Webcam Plugin up to 1.2.0 on WordPress Shortcode cross-site scripting	A vulnerability was found in React Webcam Plugin up to 1.2.0. It has been classified as problematic. Affected is an unknown function of the compo- nent Shortcode Handler. The manipulation leads to crosssite scripting. This vulnerability is traded as CVE-2023-0365. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-4652	Video Background Plugin up to 2.7.4 on WordPress Shortcode cross-site scripting	A vulnerability was found in Video Background Plugin up to 2.7.4. It has been rated as problematic. This issue affects some unknown processing of the component Shortcode Handler. The manipula- tion leads to cross-site scripting. The identification of this vulnerability is CVE-2022- 4652. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0145	Saan World Clock Plugin up to 1.8 on WordPress Shortcode cross-site scripting	A vulnerability was found in Saan World Clock Plugin up to 1.8. It has been rated as problematic. Affect- ed by this issue is some unknown functionality of the component Shortcode Handler. The manipula- tion leads to cross-site scripting. This vulnerability is handled as CVE-2023- 0145. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0370	WPB Advanced FAQ Plugin up to 1.0.6 on WordPress Shortcode cross-site scripting	A vulnerability has been found in WPB Advanced FAQ Plugin up to 1.0.6 and classified as problematic. This vulnerability affects unknown code of the com- ponent Shortcode Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023- 0370. The attack can be initiated remotely. There is no ex- ploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0364	real.Kit Plugin up to 5.1.0 on WordPress Shortcode cross-site scripting	A vulnerability classified as problematic was found in real.Kit Plugin up to 5.1.0. This vulnerability affects unknown code of the component Shortcode Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-0364. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0660	Smart Slider Plugin up to 3.5.1.13 on WordPress crosssite scripting	A vulnerability classified as problematic was found in Smart Slider Plugin up to 3.5.1.13. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-0660. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-26487	Vega lassoAppend cross-site scripting	A vulnerability which was classified as problematic has been found in Vega. This issue affects the function lassoAppend. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-26487. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-26486	Vega Scale Expression crosssite scripting	A vulnerability was found in Vega. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Scale Expression Handler. The manipulation leads to crosssite scripting. This vulnerability is known as CVE-2023-26486. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-23927	Craft CMS up to 4.3.6 Admin Dashboard cross-site scripting (GHSA-qcrj-6ffc-v7hq)	A vulnerability classified as problematic was found in Craft CMS up to 4.3.6. This vulnerability affects unknown code of the component Admin Dashboard. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-23927. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0395	menu shortcode Plugin up to 1.0 on WordPress Shortcode cross-site scripting	A vulnerability was found in menu shortcode Plugin up to 1.0. It has been declared as problematic. This vulnerability affects unknown code of the component Shortcode Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-0395. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1180	SourceCodester Health Center Patient Record Management System 1.0 hematology_print. php hem_id cross-site scripting	A vulnerability has been found in SourceCodester Health Center Patient Record Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file hematology_print. php. The manipulation of the argument hem_id leads to cross-site scripting. This vulnerability is known as CVE-2023-1180. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1179	SourceCodester Computer Parts Sales and Inventory System 1.0 Add Supplier company_name/province/city /phone_ number cross-site scripting	A vulnerability which was classified as problematic was found in SourceCodester Computer Parts Sales and Inventory System 1.0. Affected is an unknown function of the component Add Supplier Handler. The manipulation of the argument company_name/province/city /phone_number leads to cross-site scripting. This vulnerability is traded as CVE-2023-1179. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0069	WPaudio MP3 Player Plugin up to 4.0.2 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in WPaudio MP3 Player Plugin up to 4.0.2. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-0069. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0165	Cost Calculator Plugin up to 1.8 on WordPress Shortcode Attribute cross-site scripting	A vulnerability which was classified as problematic has been found in Cost Calculator Plugin up to 1.8. This issue affects some unknown processing of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-0165. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-27641	L-Soft LISTSERV prior 16.5 URL wa.exe cross-site scripting	A vulnerability was found in L-Soft LISTSERV. It has been declared as problematic. This vulnerability affects unknown code of the file wa.exe of the component URL Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-27641. The attack can be initiated remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0078	Resume Builder Plugin up to 3.1.1 on WordPress cross-site scripting	A vulnerability has been found in Resume Builder Plugin up to 3.1.1 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-0078. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0377	Scriptless Social Sharing Plugin up to 3.2.1 on WordPress Block Option cross-site scripting	A vulnerability classified as problematic was found in Scriptless Social Sharing Plugin up to 3.2.1. This vulnerability affects unknown code of the component Block Option Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-0377. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0065	i2 Pros & Cons WordPress Plugin up to 1.3.1 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in i2 Pros & Cons WordPress Plugin up to 1.3.1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to crosssite scripting. This vulnerability is known as CVE-2023-0065. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1200	ehuacui bbs username crosssite scripting	A vulnerability was found in ehuacui bbs. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument username leads to cross-site scripting. This vulnerability was named CVE-2023-1200. The attack can be initiated remotely. Furthermore there is an exploit available. This product is using a rolling release to provide continious delivery. Therefore no version details for affected nor updated releases are available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0064	eVision Responsive Column Layout Shortcodes Plugin Shortcode Attribute cross-site scripting	A vulnerability was found in eVision Responsive Column Layout Shortcodes Plugin up to 2.3. It has been classified as problematic. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-0064. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1181	icret easyimages2 up to 2.6.6 cross-site scripting	A vulnerability was found in icret easyimages2 up to 2.6.6. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1181. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0068	Product GTIN for WooCommerce Plugin up to 1.1.1 on WordPress Shortcode Attribute cross-site scripting	A vulnerability has been found in Product GTIN for WooCommerce Plugin up to 1.1.1 and classified as problematic. This vulnerability affects unknown code of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-0068. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0212	Advanced Recent Posts Plugin up to 0.6.14 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Advanced Recent Posts Plugin up to 0.6.14 and classified as problematic. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-0212. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0076	Download Attachments Plugin up to 1.2.24 on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic has been found in Download Attachments Plugin up to 1.2.24. This affects an unknown part of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-0076. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0063	Shortcodes Plugin up to 1.6.36 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Shortcodes Plugin up to 1.6.36 and classified as problematic. This issue affects some unknown processing of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-0063. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1254	SourceCodester Health Center Patient Record Management System 1.0 birthing_print.php birth_id cross-site scripting	A vulnerability has been found in SourceCodester Health Center Patient Record Management System 1.0 and classified as problematic. This vulnerability affects unknown code of the file birthing_print.php. The manipulation of the argument birth_id leads to cross-site scripting. This vulnerability was named CVE-2023-1254. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-26954	onekeyadmin 1.3.9 User Group Module cross-site scripting (ID 11)	A vulnerability which was classified as problematic was found in onekeyadmin 1.3.9. Affected is an unknown function of the component User Group Module. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-26954. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1237	answerdev answer up to 1.0.5 cross-site scripting	A vulnerability which was classified as problematic was found in answerdev answer up to 1.0.5. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1237. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1244	answerdev answer up to 1.0.5 cross-site scripting	A vulnerability classified as problematic was found in answerdev answer up to 1.0.5. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-1244. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1243	answerdev answer up to 1.0.5 cross-site scripting	A vulnerability classified as problematic has been found in answerdev answer up to 1.0.5. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1243. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-24733	PMB 7.4.6 export_ z3950_new. php cross-site scripting	A vulnerability which was classified as problematic has been found in PMB 7.4.6. Affected by this issue is some unknown functionality of the file /admin/convert /export_z3950_new.php. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-24733. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1242	answerdev answer up to 1.0.5 cross-site scripting	A vulnerability was found in answerdev answer up to 1.0.5. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-1242. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1238	answerdev answer up to 1.0.5 cross-site scripting	A vulnerability has been found in answerdev answer up to 1.0.5 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-1238. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-24737	PMB 7.4.6 Query Parameter export_ z3950.php cross-site scripting	A vulnerability has been found in PMB 7.4.6 and classified as problematic. This vulnerability affects unknown code of the file /admin/convert/ export_z3950.php of the component Query Parameter Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-24737. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-26955	onekeyadmin 1.3.9 Admin Group Module cross-site scripting	A vulnerability has been found in onekeyadmin 1.3.9 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Admin Group Module. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-26955. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1240	answerdev answer up to 1.0.5 cross-site scripting	A vulnerability was found in answerdev answer up to 1.0.5. It has been classified as problematic. Affected is an unknown function. The manipulation leads to crosssite scripting. This vulnerability is traded as CVE-2023-1240. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1197	uvdesk community up to 1.0.x cross-site scripting	A vulnerability classified as problematic has been found in uvdesk community up to 1.0. x. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1197. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1245	answerdev answer up to 1.0.5 cross-site scripting	A vulnerability which was classified as problematic has been found in answerdev answer up to 1.0.5. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-1245. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1239	answerdev answer up to 1.0.5 cross-site scripting	A vulnerability was found in answerdev answer up to 1.0.5 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-1239. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1241	answerdev answer up to 1.0.5 cross-site scripting	A vulnerability was found in answerdev answer up to 1.0.5. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-1241. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-26953	onekeyadmin 1.3.9 Add Administrator Module cross-site scripting	A vulnerability which was classified as problematic has been found in onekeyadmin 1.3.9. This issue affects some unknown processing of the component Add Administrator Module. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-26953. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2021-36713	DataTables 1.9.2 on jQuery _fnCreateCookie sBaseName cross-site scripting	A vulnerability was found in DataTables 1.9.2. It has been classified as problematic. This affects the function _fnCreateCookie. The manipulation of the argument sBaseName leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2021-36713. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1212	phpipam up to 1.5.1 cross-site scripting	A vulnerability was found in phpipam up to 1.5.1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-1212. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-26950	onekeyadmin 1.3.9 Adding Categories Module Title crosssite scripting	A vulnerability was found in onekeyadmin 1.3.9. It has been rated as problematic. This issue affects some unknown processing of the component Adding Categories Module. The manipulation of the argument Title leads to cross-site scripting. The identification of this vulnerability is CVE-2023-26950. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1275	SourceCodester Phone Shop Sales Managements System 1.0 CAPTCHA index.php cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Phone Shop Sales Managements System 1.0. This vulnerability affects unknown code of the file /osms/assets/plugins/jquery-validation- 1.11.1/demo/captcha/index.php of the component CAPTCHA Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-1275. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-26952	onekeyadmin 1.3.9 Add Menu Module cross-site scripting	A vulnerability which was classified as problematic has been found in onekeyadmin 1.3.9. Affected by this issue is some unknown functionality of the component Add Menu Module. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-26952. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1069	Complianz GDPR CCPA Cookie Consent Plugin up to 6.4.1 on WordPress GDPR / CCPA cross-site scripting	A vulnerability was found in Complianz GDPR CCPA Cookie Consent Plugin up to 6.4.1. It has been rated as problematic. This issue affects some unknown processing of the file GDPR/CCPA. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-1069. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1278	IBOS up to 4.5.5 mobil/index. php accesstoken cross-site scripting (I6G5IJ)	A vulnerability which was classified as problematic has been found in IBOS up to 4.5.5. Affected by this issue is some unknown functionality of the file mobil/index. php. The manipulation of the argument accesstoken leads to cross-site scripting. This vulnerability is handled as CVE-2023-1278. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-24657	phpipam 1.6 /subnet-masks /popup. php closeClass crosssite scripting (ID 3738)	A vulnerability classified as problematic has been found in phpipam 1.6. Affected is an unknown function of the file /subnet-masks /popup.php. The manipulation of the argument closeClass leads to cross-site scripting. This vulnerability is traded as CVE-2023-24657. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-27206	SourceCodester Best POS Management System 1.0 /kruxton/navbar.php page crosssite scripting	A vulnerability was found in SourceCodester Best POS Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /kruxton/navbar.php. The manipulation of the argument page leads to cross-site scripting. This vulnerability is handled as CVE-2023-27206. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1302	SourceCodester File Tracker Manager System 1.0 normal / borrow1.php id cross-site scripting	A vulnerability which was classified as problematic was found in SourceCodester File Tracker Manager System 1.0. This affects an unknown part of the file normal /borrow1.php. The manipulation of the argument id with the input 1"><script>alert</script> leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1302. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1286	pimcore up to 10.5.18 cross-site scripting	A vulnerability classified as problematic was found in pimcore up to 10.5.18. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-1286. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-27212	SourceCodester Online Pizza Ordering System 1.0 /php-opos /signup.php redirect cross-site scripting	A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /php-opos/signup.php. The manipulation of the argument redirect leads to cross-site scripting. This vulnerability was named CVE-2023-27212. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-27208	SourceCodester Online Pizza Ordering System 1.0 / php-opos /login.php redirect cross-site scripting	A vulnerability was found in SourceCodester Online Pizza Ordering System 1.0. It has been classified as problematic. This affects an unknown part of the file /php-opos/login.php. The manipulation of the argument redirect leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-27208. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-27211	SourceCodester Online Pizza Ordering System 1.0 /admin /navbar.php page cross-site scripting	A vulnerability was found in SourceCodester Online Pizza Ordering System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/navbar. php. The manipulation of the argument page leads to cross-site scripting. This vulnerability was named CVE-2023-27211. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2021-33351	Wyomind Help Desk Extension up to 1.3.6 on Magento Ticket Message cross-site scripting (ID 50113 / EDB-50113)	A vulnerability classified as problematic has been found in Wyomind Help Desk Extension up to 1.3.6. Affected is an unknown function of the component Ticket Message Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2021-33351. It is possible to launch the attack remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1315	osticket up to 1.16.5 cross-site scripting	A vulnerability classified as problematic was found in osticket up to 1.16.5. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-1315. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-48111	SIPE WI400 up to 11 check_login f cross-site scripting	A vulnerability classified as problematic was found in SIPE WI400 up to 11. This vulnerability affects the function check_login. The manipulation of the argument f leads to cross-site scripting. This vulnerability was named CVE-2022-48111. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1320	osticket up to 1.16.5 cross-site scripting	A vulnerability classified as problematic has been found in osticket up to 1.16.5. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1320. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1318	osticket up to 1.16.5 cross-site scripting	A vulnerability has been found in osticket up to 1.16.5 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023- 1318. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1312	pimcore up to 10.5.18 cross-site scripting	A vulnerability was found in pimcore up to 10.5.18. It has been classified as problematic. Affected is an unknown function. The manipulation leads to crosssite scripting. This vulnerability is traded as CVE-2023-1312. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1316	osticket up to 1.16.5 cross-site scripting	A vulnerability which was classified as problematic has been found in osticket up to 1.16.5. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-1316. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1319	osticket up to 1.16.5 cross-site scripting	A vulnerability was found in osticket up to 1.16.5 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-1319. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1317	osticket up to 1.16.5 cross-site scripting	A vulnerability which was classified as problematic was found in osticket up to 1.16.5. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1317. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1353	SourceCodester Design and Implementation of Covid-19 Directory on Vaccination System verification.php cross-site scripting	A vulnerability which was classified as problematic was found in SourceCodester Design and Implementation of Covid-19 Directory on Vaccination System 1.0. Affected is an unknown function of the file verification.php. The manipulation of the argument txtvaccinationID leads to crosssite scripting. This vulnerability is traded as CVE-2023-1353. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1354	SourceCodester Design and Implementation of Covid-19 Directory on Vaccination System register.php cross-site scripting	A vulnerability has been found in SourceCodester Design and Implementation of Covid-19 Directory on Vaccination System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file register. php. The manipulation of the argument txtfullname/txtage/txtaddress/txtphone leads to cross-site scripting. This vulnerability is known as CVE-2023-1354. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-23326	AvantFAX 3.3.7 cross-site scripting	A vulnerability classified as problematic was found in AvantFAX 3.3.7. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-23326. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1359	SourceCodester Gadget Works Online Ordering System 1.0 Add New User controller.php U_NAME cross-site scripting	A vulnerability has been found in SourceCodester Gadget Works Online Ordering System 1.0 and classified as problematic. This vulnerability affects unknown code of the file / philosophy/admin /user/controller.phpactionadd of the component Add New User. The manipulation of the argument U_NAME leads to cross-site scripting. This vulnerability was named CVE-2023-1359. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0073	Client Logo Carousel Plugin up to 3.0.0 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Client Logo Carousel Plugin up to 3.0.0. It has been rated as problematic. This issue affects some unknown processing of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-0073. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1372	WH Testimonials Plugin up to 3.0.0 on WordPress wh_homepage/wh_text_short /wh_text_full cross-site scripting	A vulnerability was found in WH Testimonials Plugin up to 3.0.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument wh_homepage/wh_text_short/wh_text_full leads to cross-site scripting. This vulnerability is known as CVE-2023-1372. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0844	Namaste LMS Plugin up to 2.5 on WordPress Setting cross-site scripting	A vulnerability classified as problematic was found in Namaste LMS Plugin up to 2.5. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-0844. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0066	Companion Sitemap Generator Plugin up to 4.5.1.1 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Companion Sitemap Generator Plugin up to 4.5.1.1. It has been declared as problematic. This vulnerability affects unknown code of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-0066. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-4661	Widgets for WooCommerce Products on Elementor Plugin Shortcode Attribute cross-site scripting	A vulnerability was found in Widgets for WooCommerce Products on Elementor Plugin up to 1.0.7 and classified as problematic. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-4661. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1374	Solidres Plugin up to 0.9.4 on WordPress currency_name cross-site scripting	A vulnerability was found in Solidres Plugin up to 0.9.4. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument currency_name leads to cross-site scripting. This vulnerability is handled as CVE-2023-1374. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0219	FluentSMTP Plugin up to 2.2.2 on WordPress cross-site scripting	A vulnerability which was classified as problematic has been found in FluentSMTP Plugin up to 2.2.2. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-0219. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-27093	My-Blog Post cross-site scripting	A vulnerability was found in My-Blog. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Post Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-27093. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1363	SourceCodester Computer Parts Sales and Inventory System 1.0 Add User Account username cross-site scripting	A vulnerability which was classified as problematic was found in SourceCodester Computer Parts Sales and Inventory System 1.0. Affected is an unknown function of the component Add User Account. The manipulation of the argument username leads to cross-site scripting. This vulnerability is traded as CVE-2023-1363. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-4466	Infinite Scroll Plugin prior 5.6.0.3 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in Infinite Scroll Plugin. It has been classified as problematic. This affects an unknown part of the component Shortcode Attribute Handler. The manipulation leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2022-4466. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0172	Juicer Plugin up to 1.10 on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic has been found in Juicer Plugin up to 1.10. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-0172. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-24279	Open Networking Foundation ONOS up to 2.7.0 API Documentation Dashboard url cross-site scripting	A vulnerability has been found in Open Networking Foundation ONOS up to 2.7.0 and classified as problematic. This vulnerability affects unknown code of the component API Documentation Dashboard. The manipulation of the argument url leads to cross-site scripting. This vulnerability was named CVE-2023-24279. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-26912	xenv S-mall-ssm 3d9e77f7d80289a-30f67aaba1ae73e375d33ef71 cross-site scripting (ID 37)	A vulnerability which was classified as problematic has been found in xenv S-mallssm 3d9e77f7d80289a-30f67aaba1ae73e375d33ef71. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-26912. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1418	SourceCodester Friendly Island Pizza Website and Ordering System 1.0 POST Parameter cashconfirm.php transactioncode cross-site scripting	A vulnerability classified as problematic was found in SourceCodester Friendly Island Pizza Website and Ordering System 1.0. Affected by this vulnerability is an unknown functionality of the file cashconfirm.php of the component POST Parameter Handler. The manipulation of the argument transactioncode leads to cross-site scripting. This vulnerability is known as CVE-2023-1418. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1429	pimcore up to 10.5.18 cross-site scripting	A vulnerability has been found in pimcore up to 10.5.18 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-1429. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-27711	Typecho 1.2.0 manage-comments. php cross-site scripting (ID 1539)	A vulnerability classified as problematic was found in Typecho 1.2.0. This vulnerability affects unknown code of the file /admin/manage-comments.php. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-27711. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-28106	Pimcore up to 10.5.18 crosssite scripting (GHSA-x5j3-mq9g-8jc8)	A vulnerability which was classified as problematic was found in Pimcore up to 10.5.18. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-28106. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2020-19947	Markdown Edit edit cross-site scripting (ID 12)	A vulnerability was found in Markdown Edit and classified as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument edit leads to cross-site scripting. This vulnerability is handled as CVE-2020-19947. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-27130	Typecho 1.2.0 URL Parameter cross-site scripting (ID 1535)	A vulnerability has been found in Typecho 1.2.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component URL Parameter Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-27130. The attack can be launched remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-27131	Typecho 1.2.0 cross-site scripting (ID 1536)	A vulnerability was found in Typecho 1.2.0. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-27131. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-27059	ChurchCRM 4.5.3 Edit Group cross-site scripting (ID 6450)	A vulnerability has been found in ChurchCRM 4.5.3 and classified as problematic. This vulnerability affects unknown code of the component Edit Group. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-27059. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1485	SourceCodester Young Entrepreneur E-Negosyo System 1.0 GET Parameter /bsenordering/index.php category cross-site scripting	A vulnerability classified as problematic has been found in SourceCodester Young Entrepreneur E-Negosyo System 1.0. This affects an unknown part of the file /bsenordering/index.php of the component GET Parameter Handler. The manipulation of the argument category with the input < script>alert</script> leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1485. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1481	SourceCodester Monitoring of Students Cyber Accounts System 1.0 POST Parameter index.php id cross-site scripting	A vulnerability which was classified as problematic has been found in SourceCodester Monitoring of Students Cyber Accounts System 1.0. Affected by this issue is some unknown functionality of the file modules/balance/index. phpview-balancelist of the component POST Parameter Handler. The manipulation of the argument id with the input "><script>alert</script> leads to cross-site scripting. This vulnerability is handled as CVE-2023-1481. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-24278	Squidex up to 7.3.x cross-site scripting	A vulnerability was found in Squidex up to 7.3.x. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-24278. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1515	pimcore up to 10.5.18 cross-site scripting	A vulnerability was found in pimcore up to 10.5.18. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-1515. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1517	pimcore up to 10.5.18 cross-site scripting	A vulnerability classified as problematic was found in pimcore up to 10.5.18. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-1517. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0937	VK All in One Expansion Unit Plugin prior 9.87.1.0 on WordPress $_SERVER ['REQUEST_URI'] cross-site scripting	A vulnerability classified as problematic has been found in VK All in One Expansion Unit Plugin. This affects an unknown part. The manipulation of the argument $_SERVER [&039;REQUEST_URI&039;] leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-0937. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-0273	Custom Content Shortcode Plugin up to 4.0.2 on WordPress Shortcode Attribute page/post cross-site scripting	A vulnerability was found in Custom Content Shortcode Plugin up to 4.0.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file page/post of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-0273. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0369	GoToWP Plugin up to 5.1.1 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in GoToWP Plugin up to 5.1.1. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-0369. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0167	GetResponse for Plugin up to 5.5.31 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in GetResponse for Plugin up to 5.5.31. It has been classified as problematic. Affected is an unknown function of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-0167. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1496	imgproxy up to 3.13.x cross-site scripting	A vulnerability was found in imgproxy up to 3.13.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-1496. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1536	answer up to 1.0.6 cross-site scripting	A vulnerability was found in answer up to 1.0.6 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-1536. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1535	answer up to 1.0.6 cross-site scripting	A vulnerability has been found in answer up to 1.0.6 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-1535. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1527	tsolucio corebos up to 7.x crosssite scripting	A vulnerability which was classified as problematic was found in tsolucio corebos up to 7.x. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-1527. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1572	DataGear up to 1.11.1 Plugin cross-site scripting	A vulnerability has been found in DataGear up to 1.11.1 and classified as problematic. This vulnerability affects unknown code of the component Plugin Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-1572. It is possible to launch the attack on the local host. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-24709	Paradox Security Systems IPR512 login.html cross-site scripting	A vulnerability was found in Paradox Security Systems IPR512. It has been declared as problematic. This vulnerability affects unknown code of the file login.html. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2023-24709. The attack can be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1567	SourceCodester Student Study Center Desk Management System 1.0 /admin/assign /assign.php sid cross-site scripting	A vulnerability was found in SourceCodester Student Study Center Desk Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin /assign/assign.php. The manipulation of the argument sid leads to cross-site scripting. The identification of this vulnerability is CVE-2023-1567. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1573	DataGear up to 1.11.1 Graph Dataset cross-site scripting	A vulnerability was found in DataGear up to 1.11.1 and classified as problematic. This issue affects some unknown processing of the component Graph Dataset Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-1573. The attack may be initiated remotely. Furthermore there is an exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1565	FeiFeiCMS 2.7.130201 Extension Tool slide_add.html cross-site scripting	A vulnerability was found in FeiFeiCMS 2.7.130201. It has been classified as problematic. This affects an unknown part of the file \Public\system\slide_add.html of the component Extension Tool. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-1565. It is possible to initiate the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1569	SourceCodester E-Commerce System 1.0 controller.php U_NAME cross-site scripting	A vulnerability classified as problematic was found in SourceCodester E-Commerce System 1.0. Affected by this vulnerability is an unknown functionality of the file admin /user/controller.phpactionedit. The manipulation of the argument U_NAME with the input <script>alert</script> leads to cross-site scripting. This vulnerability is known as CVE-2023-1569. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1568	SourceCodester Student Study Center Desk Management System 1.0 GET Parameter /admin/reports/index.php date_to cross-site scripting	A vulnerability classified as problematic has been found in SourceCodester Student Study Center Desk Management System 1.0. Affected is an unknown function of the file /admin/reports/index.php of the component GET Parameter Handler. The manipulation of the argument date_to leads to cross-site scripting. This vulnerability is traded as CVE-2023- 1568. It is possible to launch the attack remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-26913	EVOLUCARE ECS Imaging up to 6.21.4 new_movie.php crosssite scripting	A vulnerability classified as problematic was found in EVOLUCARE ECS Imaging up to 6.21.4. This vulnerability affects unknown code of the file new_movie.php. The manipulation leads to cross-site scripting. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability was named CVE-2023-26913. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2022-45004	Gophish up to 0.12.1 Landing Page cross-site scripting	A vulnerability which was classified as problematic has been found in Gophish up to 0.12.1. Affected by this issue is some unknown functionality of the component Landing Page. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-45004. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-28666	InPost Gallery Plugin up to 2.2.1 on WordPress add_inpost_gallery_slide_item imgurl cross-site scripting	A vulnerability which was classified as problematic was found in InPost Gallery Plugin up to 2.2.1. This affects the function add_inpost_gallery_slide_item. The manipulation of the argument imgurl leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-28666. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-24367	Temenos T24 Release genrequest.jsp routineName cross-site scripting	A vulnerability which was classified as problematic was found in Temenos T24 Release. This affects an unknown part of the file genrequest.jsp. The manipulation of the argument routineName leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2023-24367. It is possible to initiate the attack remotely. There is	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-27054	MiroTalk P2P Settings Module Name cross-site scripting (ID 139)	A vulnerability was found in MiroTalk P2P. It has been classified as problematic. Affected is an unknown function of the component Settings Module. The manipulation of the argument Name leads to cross-site scripting. This vulnerability is traded as CVE-2023-27054. It is possible to launch the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-28665	Woo Bulk Price Update Plugin up to 2.2.1 on WordPress techno_get_products page cross-site scripting	A vulnerability which was classified as problematic has been found in Woo Bulk Price Update Plugin up to 2.2.1. Affected by this issue is the function techno_get_products. The manipulation of the argument page leads to cross-site scripting. This vulnerability is handled as CVE-2023-28665. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-28664	Meta Data and Taxonomies Filter Plugin up to 1.3.0 on WordPress mdf_get_tax_options_in_widget tax_name cross-site scripting	A vulnerability classified as problematic has been found in Meta Data and Taxonomies Filter Plugin up to 1.3.0. Affected is the function mdf_get_tax_options_in_widget. The manipulation of the argument tax_name leads to cross-site scripting. This vulnerability is traded as CVE-2023-28664. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1410	Grafana up to 8.5.21/9.2.14/9. 3.10 Graphite Tooltip cross-site scripting (GHSA-qrrg-gw-7wvp76)	A vulnerability was found in Grafana up to 8.5.21/9.2.14/9.3.10. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Graphite Tooltip. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-1410. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1609	Zhong Bang CRMEB Java up to 1.3.4 save cross-site scripting (ID 12)	A vulnerability was found in Zhong Bang CRMEB Java up to 1.3.4. It has been rated as problematic. This issue affects the function save of the file /api/admin/store /product/save. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2023-1609. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-1616	XiaoBingBy TeaCMS up to 2.0.2 Arti-cle Title cross-site scripting (I6L9Z2)	A vulnerability was found in XiaoBingBy TeaCMS up to 2.0.2. It has been classified as problematic. Affected is an unknown function of the component Article Title Handler. The manipulation with the in-put < script>alert</ script> leads to cross-site scripting. This vulnerability is traded as CVE-2023-1616. It is possible to launch the attack remotely. Further-more there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1635	OTCMS 6.72 apiRun. php AutoRun mode cross-site scripting	A vulnerability was found in OTCMS 6.72. It has been declared as problematic. Affected by this vulnerabil-ity is the function AutoRun of the file apiRun.php. The manipulation of the argument mode leads to cross-site scripting. This vulnerability is known as CVE-2023-1635. The attack can be launched remotely. There is no ex-ploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0589	WP Image Carousel Plugin up to 1.0.2 on WordPress cross-site scripting	A vulnerability was found in WP Image Carousel Plugin up to 1.0.2. It has been declared as prob-lematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2023-0589. The attack can be launched remotely. There is no ex-ploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0491	Schedulicity Plugin up to 2.21 on Word-Press Shortcode Attribute cross-site scripting	A vulnerability was found in Schedulicity Plugin up to 2.21. It has been rated as problematic. This issue affects some unknown processing of the compo-nent Shortcode Attribute Handler. The manipula-tion leads to cross-site scripting. The identification of this vulnerability is CVE-2023-0491. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0823	Cookie Notice & Compliance for GDPR CCPA Plugin up to 2.4.6 on WordPress Shortcode Attribute cross-site scripting	A vulnerability classified as problematic has been found in Cookie Notice & Compliance for GDPR CCPA Plugin up to 2.4.6. This affects an unknown part of the component Shortcode Attribute Handler. The manipula-tion leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-0823. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-27241	SourceCodester Water Billing System 1.0 Add Client Module lastname cross-site scripting	A vulnerability which was classified as problematic was found in Source-Codester Water Billing System 1.0. This affects an unknown part of the com-ponent Add Client Module. The manipulation of the argument lastname leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2023-27241. It is possible to initiate the attack re-motely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-27245	File Management System 1.0.0 Edit User Module Name crosssite scripting	A vulnerability was found in File Management System 1.0.0. It has been declared as problematic. This vulnerability affects unknown code of the component Edit User Module. The manipulation of the argument Name leads to cross-site scripting. This vulnerability was named CVE-2023-27245. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1400	Modern Events Calendar Lite Plugin up to 5.16.2 on WordPress Setting cross-site scripting	A vulnerability which was classified as problematic was found in Modern Events Calendar Lite Plugin up to 5.16.2. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2023-1400. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-0272	NEX-Forms Plugin up to 8.3.2 on WordPress Shortcode Attribute cross-site scripting	A vulnerability was found in NEX-Forms Plugin up to 8.3.2 and classified as problematic. Affected by this issue is some unknown functionality of the component Shortcode Attribute Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2023-0272. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-26958	PHPGurukul Park Ticketing Management System 1.0 Admin Name cross-site scripting	A vulnerability was found in PHPGurukul Park Ticketing Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument Admin Name leads to cross-site scripting. This vulnerability was named CVE-2023-26958. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1686	SourceCodester Young Entrepreneur E-Negosyo System 1.0 GET Parameter index.php view cross-site scripting	A vulnerability was found in SourceCodester Young Entrepreneur ENegosyo System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file bsenordering /admin/category/index.php of the component GET Parameter Handler. The manipulation of the argument view with the input <script>alert</script> leads to cross-site scripting. The identification of this vulnerability is CVE-2023-1686. The attack may be initiated remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-26982	polonel Trudesk 1.2.6 Create Ticket Add Tags cross-site scripting	A vulnerability was found in polonel Trudesk 1.2.6. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Create Ticket Handler. The manipulation of the argument Add Tags leads to cross-site scripting. This vulnerability is handled as CVE-2023-26982. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.
CVE-2023-1771	SourceCodester Grade Point Average GPA Calculator 1.0 Master.php get_scale perc crosssite scripting	A vulnerability was found in SourceCodester Grade Point Average GPA Calculator 1.0 and classified as problematic. Affected by this issue is the function get_scale of the file Master.php. The manipulation of the argument perc leads to cross-site scripting. This vulnerability is handled as CVE-2023-1771. The attack may be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

XML External Entity Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2023-27480	XWiki Platform prior 13.10.11 /14.4.7/14.10-rc-1 XAR Import xml external entity reference (GHSA-gx4f-976g- 7g6v)	A vulnerability was found in XWiki Platform. It has been classified as problematic. Affected is an unknown function of the component XAR Import Handler. The manipulation leads to xml external entity reference. This vulnerability is traded as CVE-2023-27480. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as Cross-Site Scripting attack.

Indusface is a leading application security SaaS company that secures critical Web, Mobile & API applications of 5000+ global customers using its award-winning fully managed platform that integrates a web application scanner, web application firewall, DDoS &, BOT Mitigation, CDN, and threat intelligence engine. The company has been funded by Tata Capital Growth Fund, is Great Place to Work certified, mentioned by analysts like Gartner, Forrester, etc in their reports, and has been the recipient of many awards such as the Economic Times Top 25, NASSCOM DSCI Top Security Company, Deloitte Asia Top 100 , and several other such prestigious recognitions.

CONTACT US - +91 265 6133021 | +1 866 537 8234
EMAIL - sales@indusface.com

Indusface is the only cloud WAAP (WAF) vendor with 100% customer recommendation for 3 consecutive years

A Customers' Choice for 2022 and 2023 Gartner® Peer Insights™